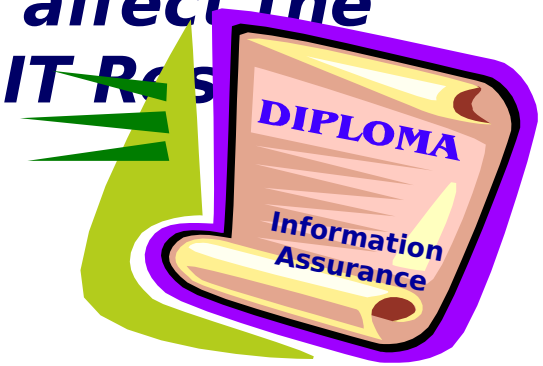
# Information Assurance (IA) Basic User Training 14 MAY 2009

# The A B C's of Computer Security

- ***Purpose:*** *To ensure all users of Navy Information Technology (IT) Resources have a basic understanding of their Information Assurance responsibilities. To increase Navy wide awareness of the implications or vulnerabilities that may occur from their actions. Whether the intent is innocent or malicious, risky behaviors may affect the security posture of the Navy's IT Re*




***See notes appended to slides for references and additional information related to the slide****

***Guaranteeing "Smart Users" for Navy IT Resources!!!***

# Defense In Depth

- *Navy and DoD implement a layered defense strategy to protect our networks and the information carried on them.*
- *Defense in Depth requires several elements:*
  - *People – Written policies, training, incident response teams*
  - *Processes – Management oversight, commitment of resourced budget, contingency planning*
  - *Technology – Firewalls, public key infrastructure, Anti-Virus protection, integrity assurances.*

# Applicability

- ***ALL* active duty, civil service, contractor and/or a foreign national personnel who have been granted access to or who are providing services for Navy IT Resources are required to comply with the Navy's Information Assurance (IA) Program.**

***No one is exempt from practicing good IT security habits!***

# IA Training Is Required

- ***New users will be provided basic IA training <u>prior to</u> obtaining access to Navy IT Resources***

  ***(This training meets that requirement)***

- ***All Commanding Officers and Officers In Charge will provide (at a minimum) annual IA training to all users. This training will be provided and tracked via Navy Knowledge Online (NKO).***
  - ***Users not authorized NKO access (e.g., F/N's) will be tracked by command.***
- ***User training is a vital part of a successful Defense In Depth strategy.***

***https://wwwa.nko.navy.mil/portal/splash/index.jsp***

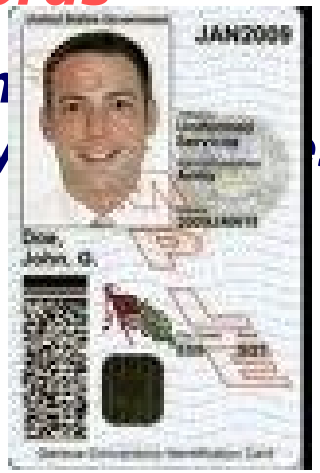
# Protecting Information & IT Resources

- *Users will take necessary actions to safeguard information and prevent IT Resources from modification, tampering, destruction or unauthorized access/use.*
- *All information and Navy IT Resources shall be properly marked/labeled to easily and quickly identify the appropriate classification. Information that resides and is processed on classified systems shall be properly marked and safeguarded per SECNAV M-5510.36.*

***The Network is a weapons system and should be protected as such!***

# CRYPTOGRAPHIC LOG ON (CLO)

- **DoD is moving aggressively towards Cryptographic Log On (CLO) in lieu of individual passwords**
  - **All authentication to unclassified DoD networks must be performed using DoD Public Key Infrastructure (PKI)**
  - **CLO enhances security and it also means that users don't have to remember passwords**
  - **Accounts that can't use CLO at this tim… rity …s**



# Creating Good Passwords

- **Navy IT Resources require a unique ID and password that shall be protected at the same classification level as the system itself** *(System classification = SECRET means Password = SECRET)*
- **Creating a "good password" means that your password cannot be easily guessed or cracked**
  - *At a minimum, a case sensitive 14-character mix of upper/lower case letters, numbers, and special characters, including at least one of each*
  - *Should be a phrase that can be repeated when logging in (Password "lie2casp,bCL0ie!" = It is easy to create a safe password, but CLO is easier!)*
  - *Do not use common words (Family names, dictionary words, birth dates, anniversary etc)*
  - *Do not use keyboard walks (e.g. Qwer^789 or Abcd!234)*
- **DO NOT share your password with others!**

**DO NOT write down your password and leave it near system!!!!**

# Protecting Your Workstation

- When leaving your work area, be sure and lock your screen with a password/CLO protected screensaver OR if you are going to be away for long periods of time…LOG OFF!
- Shut down your computer at the end of each day unless otherwise directed by your command IAM or higher authority guidance (e.g., NETWARCOM direction)
  - Power Mgmt (Also turn off monitor/printer to conserve electrical power)
- Ensure your workstation has a password protected screensaver that automatically activates after a period of time.

# Viruses, Worms & Malicious Code

- *Users need to ensure the system they are using has virus scanning software that automatically updates!*
- *When you access or import attachments, you are required to scan the documents for viruses or malicious code.*
  - *(If the system does not do the scan automatically, scan must be done by the user manually)*
  - *NMCI is configured to scan for viruses or malicious code automatically on local machine and on external devices (CD, Floppy, Thumb Drive etc) when read/write occurs.*
  - *If you are uncertain as to your network[illegible] configuration, seek guidance from your command IA*

# Accessing Classified or Controlled Unclassified Information on IT systems

- **Users shall:**
  - only be granted access to a classified system, if they hold the requisite level of clearance and a valid "need to know."
  - Properly mark, safeguard, disseminate, and transmit all classified and Controlled Unclassified Information per SECNAV M-5510.36
  - Be aware that misuse of Navy IT systems is a potentially disqualifying factor for obtaining or retaining a security clearance (SECNAV M-5510.30, Appendix G applies).

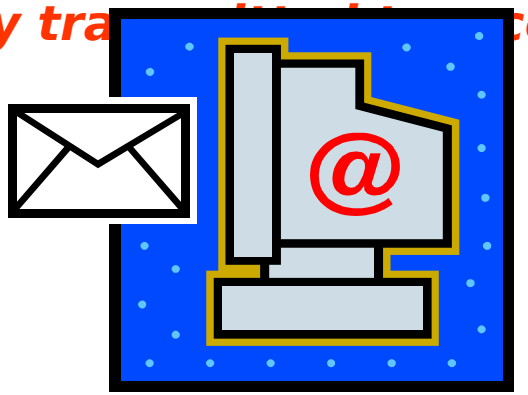
**Misuse of Navy IT is grounds for revoking security clearance!!!**

# Safeguarding Personally Identifiable Information

- *Loss of this type of information may lead to identity theft or other fraudulent use of the information*
  - *Individuals charged with maintaining this type of information have a special duty to protect that information from loss and misuse*
  - *OMB memo (22MAY06) directs Heads of Departments and Agencies to remind employees of:*
    - *Their specific responsibilities for safeguarding personally identifiable information*
    - *Rules for acquiring and using such information*
    - *Penalties for violating these rules*
  - *All hands are encouraged to review Privacy Act 103*
    - *Training slides posted on Infosec Website (see notes)*

# Email

- **Each user is given a Navy email account. Accessing commercial web-based email from Navy IT Resources is not authorized.**
  ***(Web-based e-mail bypasses anti-virus scanning and creates an unacceptable security risk.)***
- **Auto-forwarding of official email to a commercial email account is prohibited.**
  ***(Complying with this eliminates the possibility of Classified or Controlled Unclassified Information (CUI) being improperly tra commercial source.)***



# Digitally Signed Email

- Digital signatures provide identification of the sender & assurance that the data was unchanged
  - Helps to prevent socially engineered (Phishing) emails
- Users should only trust emails with DoD signatures
- Digitally sign all emails that contain

**General Rule**

**If the email contains any official business…**

**SIGN IT!**

# Encrypted Email

- *Encrypting email using DoD PKI ensures that the data may only be read by authorized individuals*
- *Encrypt all email that contains Controlled Unclassified Information (CUI), For Official Use Only (FOUO), Personally Identifiable Information (PII), Privacy Act data, Health Insurance Portability and Accountability Act (HIPAA) information, etc.*
- *Use https://dod411.gds.disa.mil to find encryption certificates for DoD users*

# Other Forms of Misuse

- **Other actions that are prohibited unless specifically authorized by the Local Information Assurance Authority or DAA are:**
  - **By-passing security mechanisms or architecture that have been put in place to prevent or isolate access or privileges.**
  - **Introducing or using unauthorized software or hardware on a Navy IT system.**
  - **Moving, relocating or changing configuration of any software or hardware on or in a Navy IT system.**
  - **Use of personally owned software or hardware.**
  - **Participating in any action that causes a disruption or denial of service.**
  - **Uploading executable files (e.g., .exe, .com, .vbs, or .bat)**
  - **Writing, coding, compiling, storing, transmitting, transferring, or introducing malicious software, programs, or code.**

**NOT ALLOWED!!!**

# Inappropriate Use of Navy IT Resources

- **Never use Navy IT Resources for:**
  - Actions that would reflect adversely on the Navy or DOD.
  - Pornography, chain letters, unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use.
  - Violation of a statute or regulation.
  - Inappropriately handled classified information.
  - Other uses [illegible] incompatible with public service.

# CONSENT TO MONITORING

- **All users are reminded of the DoD banner, which appears at every logon:**
  - *You are accessing a U.S. government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes security measure (e.g., authentication and access controls) to protect USG interests–not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User agreement for details.*
- **As users, you understand that:**
  - *You are subject to monitoring*
  - *There is no expectation or right to privacy over the data and communications generated through your use*

# Who Can You Call for Help??

- *Each command has a local Information Assurance Manager (IAM) or Information Assurance Officer (IAO) who can assist you if you have questions or concerns related to protecting Navy IT Resources.*
- *If you suspect or are aware of any event, incident or action that could impact the operations of Navy IT Resources contact your command IAM/IAO immediately*

***Make it a point to know who your command/unit IAM/IAO is!!!***

# In a Nutshell……

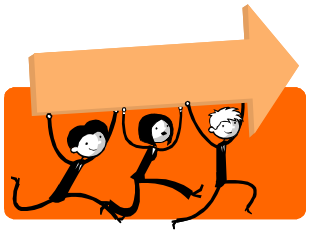
- ***YOU have been granted a privilege to be able to access Navy IT Resources…but along with that comes responsibility. Do not take safeguarding the Navy's IT Resources or information lightly. YOU are the first link in the chain for achieving a Navy Enterprise Network that is secure and available…don't be the weak link!***

***TAKE YOUR RESPONSIBILITY AS A NAVY IT RESOURCE USER SERIOUSLY!***

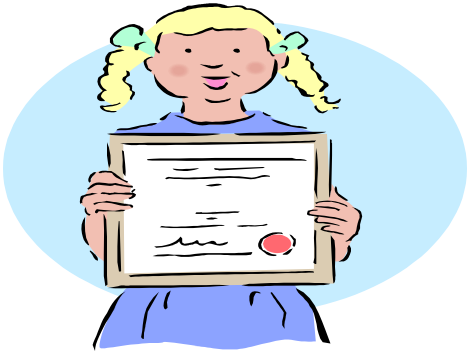
# The Finish Line……

**The information in this training provides the responsibilities you acknowledge when you sign OPNAV 5239/14 – System Authorization Access Request NAVY (SAAR-N)**

Good Training



Equals



A Responsible Computer User

# QUESTIONS????

***Contact your command IAM Gary Leischner or IAO ITC(SW) Eric Purcell if you have questions concerning this briefing or if you need additional information***

***Visit https://infosec.navy.mil for additional information and policy documents***